

**TRANSMITTAL OF APPEAL BRIEF (Large Entity)**Docket No.  
ITL.0506US

In Re Application Of: Larry H. Gass, et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/922,041	August 3, 2001	Minh Dieu T. Nguyen	47795	2137	7270

Invention: Firmware Security Key Upgrade Algorithm

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:  
**December 18, 2007**

The fee for filing this Appeal Brief is: No fee due; fee paid on 10/25/2006.

- ☐ A check in the amount of the fee is enclosed.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 20-1504. I have enclosed a duplicate copy of this sheet.
- ☐ Payment by credit card. Form PTO-2038 is attached.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

Dated: December 19, 2007

---

*Signature*

Timothy N. Trop, Reg. No. 28,994  
TROP, PRUNER & HU, P.C.  
1616 S. Voss Road, Suite 750  
Houston, TX 77057  
713/468-8880 [Phone]  
713/468-8883 [Fax]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

December 19, 2007

(Date)

  
*Signature of Person Mailing Correspondence***Nancy Meshkoff***Typed or Printed Name of Person Mailing Correspondence*

CC:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:

Larry H. Gass, et

Serial No.: 09/922,041

Filed: August 3, 2001

For: Firmware Security Key  
Upgrade Algorithm

Art Unit: 2137

Examiner: Minh Dieu T. Nguyen

Atty Docket: ITL.0506US  
(P10475)

Assignee: Intel Corporation



Mail Stop **Appeal Brief-Patents**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF**

Date of Deposit: December 19, 2007

I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

  
Nancy Meshkoff

## **TABLE OF CONTENTS**

REAL PARTY IN INTEREST .....	3
RELATED APPEALS AND INTERFERENCES.....	4
STATUS OF CLAIMS .....	5
STATUS OF AMENDMENTS .....	6
SUMMARY OF CLAIMED SUBJECT MATTER .....	7
GROUND OF REJECTION TO BE REVIEWED ON APPEAL .....	10
ARGUMENT.....	11
CLAIMS APPENDIX.....	13
EVIDENCE APPENDIX.....	16
RELATED PROCEEDINGS APPENDIX .....	17

**REAL PARTY IN INTEREST**

The real party in interest is the assignee Intel Corporation.

**RELATED APPEALS AND INTERFERENCES**

None.

### **STATUS OF CLAIMS**

Claims 1, 3-7, 27, 29, and 32-42 (Rejected).

Claims 2, 8-26, 28, and 30-31 (Canceled).

Claims 1, 3-7, 27, 29, and 32-42 are rejected and claims 1, 3-7, 27, 29, 32, and 40-42 are the subject of this Appeal Brief.

### **STATUS OF AMENDMENTS**

No reply was filed after the Final Rejection of 11/16/2007. All amendments have therefore been entered.

## SUMMARY OF CLAIMED SUBJECT MATTER

In the following discussion, the independent claims are read on one of many possible embodiments without limiting the claims:

1. A method comprising:
  - identifying (Fig. 3, 304) a firmware upgrade request by a firmware program (specification, page 9, lines 11-17);
  - retrieving a file signed with a private key (Fig. 3, 314; specification, page 9, lines 18-24);
  - validating the file with a public key (Fig. 3, 316; specification, page 9, lines 25-27);
  - upgrading a portion of the firmware program by the firmware program (Fig. 3, 322; specification, page 10, lines 6-10);
  - locking a device storing the firmware program such that a second portion of the firmware program is not readable (Fig. 3, 308; specification, page 8, line 25-page 9, line 2);
  - validating the public key (Fig. 3, 316; specification, page 9, lines 18-22); and
  - retrieving a second public key from the firmware program if the public key is not valid (Fig. 3, 318; specification, page 9, lines 23-24).

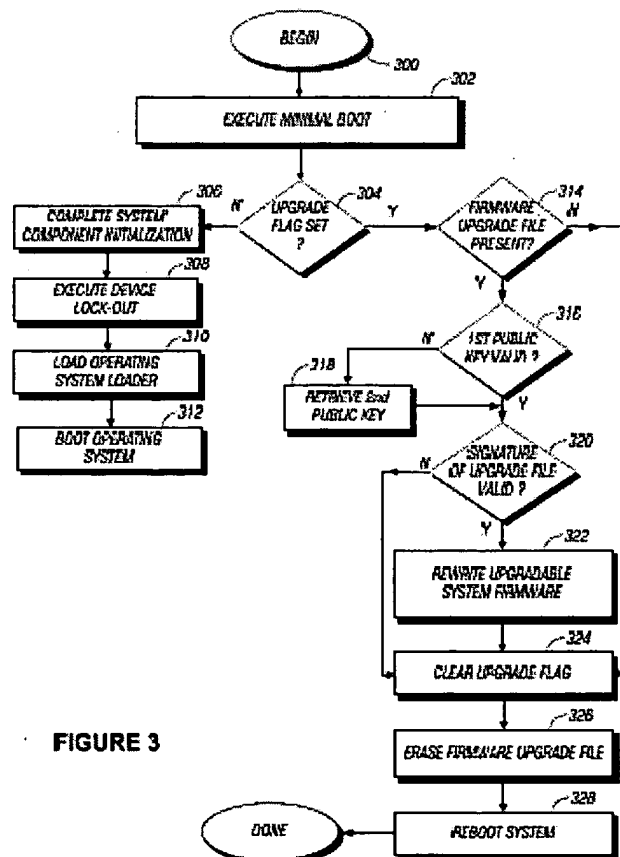


FIGURE 3



4. The method of claim 3, further comprising:

deleting the file (Fig. 3, 326; specification, page 13, lines 11-16); and  
clearing the flag (Fig. 3, 324, specification, page 10, lines 11-12).

27. An article comprising a medium storing instructions for enabling a processor-based system to:

identify (Fig. 3, 304) a firmware upgrade request by a firmware program  
(specification, page 9, lines 11-17);

retrieve a file signed with a private key (Fig. 3, 314; specification, page 9, lines 18-24);

validate the file with a public key (Fig. 3, 316; specification, page 9, lines 25-27);  
upgrade a portion of the firmware program by the firmware program (Fig. 3, 322;  
specification, page 10, lines 6-10);

lock a device storing the firmware program such that the public key is not readable  
(Fig. 3, 308; specification, page 8, line 25-page 9, line 2);

validate the public key (Fig. 3, 316; specification, page 9, lines 18-22); and

retrieve a second public key from the firmware program if the public key is not valid  
(Fig. 3, 318; specification, page 9, lines 23-24).

32. A method comprising:

identifying (Fig. 3, 304) a firmware upgrade request by a firmware program  
(specification, page 9, lines 11-17);

retrieving a file signed with a private key (Fig. 3, 314; specification, page 9, lines 18-24);

validating the file with a public key (Fig. 3, 316; specification, page 9, lines 25-27);  
upgrading a portion of the firmware program by the firmware program (Fig. 3, 322;  
specification, page 10, lines 6-10);

locking a device storing the firmware program such that a second portion of the  
firmware program is not readable (Fig. 3, 308; specification, page 8, line 25-page 9, line 2);

validating the public key (Fig. 3, 316; specification, page 9, lines 18-22);

retrieving a second public key from the firmware program if the public key is not valid (Fig. 3, 318; specification, page 9, lines 23-24);

reading a flag, wherein the flag is located in a non-volatile medium (Fig. 1, 46) (Fig. 3, 304; specification, page 8, lines 19-21);

determining that the flag is set;

deleting the file (Fig. 3, 326; specification, page 13, lines 11-16); and

clearing the flag (Fig. 3, 324, specification, page 10, lines 11-12).

40. A processor-based system comprising:

a processor (Fig. 1, 48); and

a storage (Fig. 1, 40) storing a basic input/output system (Fig. 1, 200), said basic input/output system including a first portion (Fig. 1, 10) that is not upgradable and a second portion (Fig. 1, 20) that is upgradable, said first portion including an upgrade verification code (Fig. 2, 14) (specification, page 4, lines 23-27).

41. The system of claim 40 including a public key (Fig. 2, 28) in said first portion (Fig. 2, 20).

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

**GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

- A. Whether claim 40 is anticipated under 35 U.S.C. § 102(e) by Sudia (U.S. Patent Application Publication No. 2001/0050990).**
- B. Whether claims 1, 3, 5-7, 27, and 29 are unpatentable under 35 U.S.C. § 103(a) over Angelo (U.S. Patent No. 5,748,940) in view of Falik (U.S. Patent Application Publication No. 2002/0166061) and further in view of Sudia.**
- C. Whether claim 4 is unpatentable under 35 U.S.C. § 103(a) over Angelo in view of Falik, in view of Sudia, and further in view of Toft (U.S. Patent Application Publication No. 2002/0138592).**
- D. Whether claims 41-42 are unpatentable under 35 U.S.C. § 103(a) over Sudia in view of Falik.**

## **ARGUMENT**

**A. Is claim 40 anticipated under 35 U.S.C. § 102(e) by Sudia (U.S. Patent Application Publication No. 2001/0050990)?**

Claim 33 calls for providing information for authenticating an upgrade of a second portion of firmware code, in a first portion of firmware code. The first portion includes firmware code that is not upgradeable, while the second portion includes firmware code that is upgradeable.

The only cited reference to Sudia has nothing about where any authenticating information is stored. Therefore, as a matter of law, the reference is insufficient to support the rejection.

Three different things in Sudia have been cited in the office action. The Abstract has been carefully reviewed and there is nothing therein about where the authentication data might be stored relative to the two different memory areas. Paragraph 76 has been carefully reviewed and, while there is a discussion of different memory areas, there is nothing that indicates that the information for authenticating an upgrade of the second portion is contained in the non-upgradeable first portion. Also cited is paragraph 99 which simply has four words, none of which have anything to do with the claimed invention. Finally, paragraph 248 is cited which then talks about different areas of memory, but never indicates where any authentication information is stored.

Therefore a *prima facie* rejection of claim 33 is not made out.

For the same reason, claims 40-42 should be allowable.

**B. Are claims 1, 3, 5-7, 27, and 29 unpatentable under 35 U.S.C. § 103(a) over Angelo (U.S. Patent No. 5,748,940) in view of Falik (U.S. Patent Application Publication No. 2002/0166061) and further in view of Sudia?**

Claim 1 calls for retrieving a second key from a firmware program if the public key is not valid. The Examiner suggests that this is met by some backup key. But the backup key is not obtained if the public key is not valid.

For the same reason, claim 27 and its dependent claims should be in condition for allowance.

**C. Is claim 4 unpatentable under 35 U.S.C. § 103(a) over Angelo in view of Falik, in view of Sudia, and further in view of Toft (U.S. Patent Application Publication No. 2002/0138592)?**

For the reasons set forth in sections A and B, these rejections should also be reversed.

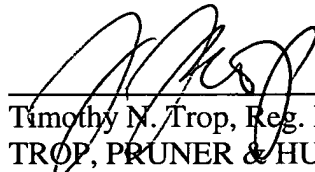
**D. Are claims 41-42 unpatentable under 35 U.S.C. § 103(a) over Sudia in view of Falik?**

On the same basis as set forth in section A above, claim 34 should be in condition for allowance. Claims 35-39 should, likewise, be allowable.

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

Date: December 19, 2007



---

Timothy N. Trop, Reg. No. 28,994  
TROP, PRUNER & HU, P.C.  
1616 S. Voss Road, Suite 750  
Houston, TX 77057  
713/468-8880 [Phone]  
713/468-8883 [Fax]

Attorneys for Intel Corporation

## **CLAIMS APPENDIX**

The claims on appeal are:

1. A method comprising:
  - identifying a firmware upgrade request by a firmware program;
  - retrieving a file signed with a private key;
  - validating the file with a public key;
  - upgrading a portion of the firmware program by the firmware program;
  - locking a device storing the firmware program such that a second portion of the firmware program is not readable;
  - validating the public key; and
  - retrieving a second public key from the firmware program if the public key is not valid.
3. The method of claim 1, identifying a firmware upgrade request by a firmware program further comprising:
  - reading a flag, wherein the flag is located in a non-volatile medium; and
  - determining that the flag is set.
4. The method of claim 3, further comprising:
  - deleting the file; and
  - clearing the flag.
5. The method of claim 1, further comprising:
  - determining that the file is not authentic; and
  - locking the device.
6. The method of claim 1, further comprising:
  - locking the device after upgrading a portion of the firmware program by the firmware program.

7. The method of claim 1, wherein the second portion of the firmware program is a public key.

27. An article comprising a medium storing instructions for enabling a processor-based system to:

identify a firmware upgrade request by a firmware program;

retrieve a file signed with a private key;

validate the file with a public key;

upgrade a portion of the firmware program by the firmware program;

lock a device storing the firmware program such that the public key is not readable;

validate the public key; and

retrieve a second public key from the firmware program if the public key is not valid.

29. The article of claim 27, further storing instructions that enable the processor-based system to:

determine that the file is not authentic; and

lock the device.

32. A method comprising:

identifying a firmware upgrade request by a firmware program;

retrieving a file signed with a private key;

validating the file with a public key;

upgrading a portion of the firmware program by the firmware program;

locking a device storing the firmware program such that a second portion of the firmware program is not readable;

validating the public key;

retrieving a second public key from the firmware program if the public key is not valid;

reading a flag, wherein the flag is located in a non-volatile medium;

determining that the flag is set;  
deleting the file; and  
clearing the flag.

40. A processor-based system comprising:  
a processor; and  
a storage storing a basic input/output system, said basic input/output system including a first portion that is not upgradable and a second portion that is upgradable, said first portion including an upgrade verification code.

41. The system of claim 40 including a public key in said first portion.

42. The system of claim 40 including two public keys in said first portion.



## **EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.